(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 647 925 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **94307376.7**

(51) Int. Cl.[6] : **G07B 17/04**

(22) Date of filing : **07.10.94**

(30) Priority : **08.10.93 US 133398**

(43) Date of publication of application :
12.04.95 Bulletin 95/15

(84) Designated Contracting States :
CH DE FR GB LI

(71) Applicant : **PITNEY BOWES, INC.**
World Headquarters
One Elmcroft
Stamford Connecticut 06926-0700 (US)

(72) Inventor : **Pintsov, Leon A.**
365 Mountain Road
W. Hartford, Connecticut 06107 (US)
Inventor : **Connell, Richard A.**
24 Lower Salem Road
South Salem, New York, 10590 (US)
Inventor : **Sansone, Ronald P.**
4 Trails End Road
Weston, Connecticut 06883 (US)
Inventor : **Schmidt, Alfred C.**
201 Branch Brook Road
Wilton, Connecticut 06897 (US)

(74) Representative : **Cook, Anthony John et al**
D. YOUNG & CO.
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Postal rating system with verifiable integrity.

(57) A data center provides a rate table to a user. The rate table is communicated to the mailer along with a hash code. The hash code is based on information from the rating table. The hash code provides a unique number based on the rating table provided. The algorithm within a secure device and to which the rate table is loaded regenerates the hash code based on the information received from the rate table and compares the transmitted hash code with the generated hash code. A comparison is made of the received hash code and the generated hash code to verify that the rate table data has not been intentionally or unintentionally corrupted. The transmitted hash code may be encrypted by the data center and when received decrypted by the mailer. The encryption decryption process establishes authenticity of the data center if desired.

The generation of a hash code based on the stored rate table and a comparison with a stored hash code previously transmitted can be initiated prior to postage printing and used to insure proper rating. Printing is enabled only after the rating process has been properly implemented. The hash code and rating information may be printed on the mail piece such that a verifying party can reconstruct the rating process and determine if rating inaccuracy occurred. Various rating inaccuracy for a particular user can be stored by the verifying party to detect a recurrence of rating errors. Rating profiles for particular users or group of users may be stored to enable generation of user profiles.

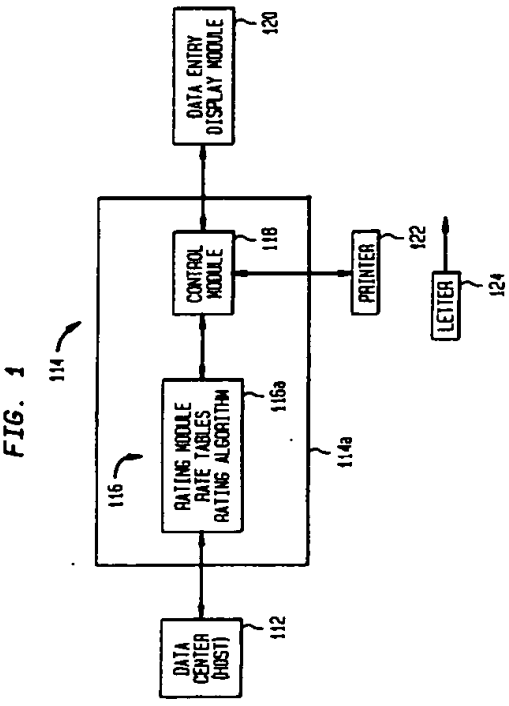


FIG. 1

EP 0 647 925 A2

date of the postage imprint. The code may be printed in encrypted form on the mail piece and the encrypted code may be printed along with other encrypted information on the mail piece. Alternatively the hash code may be combined with other information such as the postal value and postage evidencing device identification and the combined result then encrypted and printed on the mail piece.

In accordance with yet another feature of the embodiments the rating inaccuracies for a particular user can be stored by the verifying party to detect a recurrence of rating errors and to automatically initiate appropriate corrective and/or other actions should, for any given mailer or group of mailers, rating errors of particular categories exceed certain threshold levels.

In accordance with still another feature of the embodiments the rating profile for a particular user or a group of users is stored by the verifying party to enable the generation of a profile of a mailer or a group of mailers to provide business data for marketing to such mailer further postal services and/or informational reports based upon verified mailing patterns, such as rate, level of service, mail destination, distribution and the like.

Preferred embodiments of the present invention will now be described with reference to the following figures wherein like reference numerals designate similar elements in the various views and in which:

FIGURE 1 is a mailing system employing a secure rating module allowing verifiable rating integrity;

FIGURE 2 is a flow chart of the activities of the data center involved with transmitting to a secure rating module a rate table in accordance with the present invention;

FIGURE 3 are the activities at the postal evidencing device involved with processing a received rate table and the process by which verification of the integrity of the rate table data and the authenticity of the data center is established in the postage evidencing device;

FIGURE 4 is a flow chart within the postage evidencing device for rating a mail piece and printing the appropriate Postal Revenue Block on the mail piece;

FIGURE 5 is a flow chart of a sub routine within the Authenticate Rate Table and Rate Computation Algorithm block of FIGURE 4; and,

FIGURE 6 is an imprint on a mail piece in accordance with the present invention.

General Overview

The postage value (rate) for every mail piece may be encrypted together with other data to generate a digital token. A digital token is encrypted information that helps to authenticate the value or other information imprinted or to be imprinted on a mail piece. Examples of systems for generating and using digital tokens are described in U.S. Patent No. 4,757,537 for SYSTEM FOR DETECTING UNACCOUNTED FOR PRINTING IN A VALUE PRINTING SYSTEM; U.S. Patent No. 4,831,555 for UNSECURED POSTAGE APPLYING SYSTEM; and U.S. Patent No. 4,775,246 for SYSTEM FOR DETECTING UNACCOUNTED FOR PRINTING IN A VALUE PRINTING SYSTEM. The entire disclosure of these three patents is hereby incorporated herein by reference.

As a result of the digital token incorporating encrypted postage value, altering of the printed postage value in a postal value revenue block is detectable by a standard verification procedure. Thus, to underpay postage, an attempt may be made to interfere with the rating process (as opposed to the resulting printed postage value).

Rating with verifiable integrity in accordance with the system described herein helps to: 1) provide diagnostics to the party conducting verification to enable detection of inadvertent misrating of mail pieces; and 2) provide evidence to the party conducting verification of deliberate underrating of mail pieces.

Rating input parameters may be entered into a system manually or automatically or partially manually and partially automatically. For example, sensory data such as weight, size of mail pieces and presence of a barcode can be automatically entered while desired level of service or mail class can be keyed in manually or entered by default from a file. Alternatively all rating parameters can be entered into the system manually. The process of computing the postal value (or rate) is based on calculations involving input rating parameters and a rate table. The process of mail rating, however, can produce incorrect results. The following are such examples:

A) Entered incorrect rating parameter or parameters (e.g. wrong entered weight or size).

B) The rate table is obsolete or the wrong rate table.

C) The rate table is incorrect because it has been deliberately altered.

D) Entered input rating parameter or parameters are incorrect and the rate table is obsolete or incorrect.

E) Entered input rating parameter or parameters are incorrect and the rate table has been deliberately altered.

It should, of course, be recognized that the above examples can be combined to produce additional examples such as A and B or A and C or B and C or A and B and C.

The case of inadvertent misrating can occur due to incorrectly entered data, or obsolete or incorrect rate table or both. In the above examples, the case of inadvertent misrating is equivalent to examples A, B or D. In

HAVING PLURAL COMPUTING SYSTEMS; other types of metering system for evidencing postage such as, for example, as disclosed in U.S. Patent No. 4,757,537 for SYSTEM FOR DETECTING UNACCOUNTED FOR PRINTING IN A VALUE PRINTING SYSTEM: or U.S. Patent No. 4,934,846 for FRANKING SYSTEM. The postage evidencing device (which may be a personal computer type metering system, however) should preferably have the ability to print variable information on a mail piece to provide the requisite information for verification by a verifying authority as will be hereinafter explained.

The postage evidencing device 114 includes a rating module 116. The rating module stores the rate tables which are communicated to the the postage evidencing device from the data center 112. The rating module 116 is operatively connected to a control module 118 which would include a central processing unit and various other suitable electronic components and program control devices such as programmable read only memories (PROMs), random access memories (RAMs) and non-volatile memories (NVMs) for storing various postal and accounting data. Many system architectures are suitable for the present invention. For example, the accounting circuitry and NVM(s) can be part of the rating module within the secure housing 116a (tamper resistant device housing) or within a separate secure housing. The housing 114a may be a secure housing, or distributed processing systems may be employed.

A data entry module 120 is provided to allow a user to enter information into the postage evidencing device 114. This data may include, for example, the weight, size, class of service and other data concerning the mail piece and relevant to the rating and mail finishing processes. Examples of the types of data that can be entered by a user includes mail class, weight, dimension (length, width, or thickness or all of them), desired service level, work share level (for the United States Postal Service these may include indication of due presence of certain bar code, ZIP code, or ZIP + 4 code, ZONE code or presort level, etc.). Yet another type of data that could be entered could be, for example, a graphics code for the graphics to be printed. It should be recognized that any other factors that are deemed to be relevant by a particular postal service carrier in the rating process may be enterable by the user through the data entry module 120. The entry can be manual or automatic; the data may be from a computer system associated with creating or tracking the mail pieces or it may be scanned or measured from the mail piece itself. A printer 122 such as a thermal printer or ink jet printer or pin printer or laser printer is coupled to the control module.

It should be recognized that the rating process can be viewed as mapping of a set of input parameters (which can be called a vector) into a set of rational numbers which represents the postal rates. This can be viewed as mapping f from a set of input vectors {I} into a set of numbers **R** which represents the postal rates. As an example, the input vector (that can consist of such components as: a) two ounce weight category, b) zone three, and c) a size indicator) can be mapped into a unique and specific rate, for example, 43 cents. As each of the vector components change, the rate changes. If the size indicator is eliminated and the mail piece was not, for example, oversized, the rate, for example, could diminish to a lower rate. A further example would be a one ounce letter with no zone category and no oversize category and no presort or other worksharing that would yield still a different rate. Thus, the various vectors (rating parameters) which constitute the input for the rate table determine the rate. As vectors change the rates may go up or down depending on the particular rate table involved. These parameters for rating vary from postal service to postal service and carrier to carrier. The rating parameters can be any number of parameters depending applicable rating criteria. These rating parameters will lead ultimately to a single price that is to be paid as determined by the appropriate rate table. Thus, input "vectors" can be utilized as the rate table input to map onto the rate table in the postage evidencing device or system rating module to establish the actual postage to be imprinted on the mail piece. It should be specifically recognized that the establishing of the postal value to be imprinted on a mail piece may require the utilization of more than one rate table. For example, a rate table may exist for delivery charges, and a separate rate table for mail piece insurance charges.

Another explanation of how the rating process can be viewed as a mapping from a set of input vectors {I} into a set of numbers **R** which represent postal rates is as follows: An input vector is an ordered set of numerical parameters:

$$I = (a_1, a_2, \ldots, a_n)$$

where

a_1 is the weight of the mail piece,

a_2 is the length of the mail piece,

a_3 is the width of the mail piece,

a_4 is the thickness of the mail piece,

a_5 is the desired level of service (including delivery time, special processing request such as registered mail etc.)

a_6 is a postal code of the origination address

The data center would operate to send a rate table to a postage evidencing device via a communications channel (phone line or other transmission). The secret information (for example, a secret key in a case of a secret key based protocol) is stored both at the data center and in the postage evidencing device. Alternatively, in a public key system one of the parties (for example, the data center) knows a secret key, and the other party (here, the postage evidencing device) knows a matching public key. The protocol for mutual authentication requires that the data center first sends information in plain text and then the same information encrypted with its secret key. The postage evidencing device upon receipt of both messages deciphers the encrypted message with its secret (or public)key and compares it with its plain text version. If a match is made, the data sender is authenticated, since only the sender knew the secret key. Similarly, the postage evidencing device can send two messages, plain text and encrypted message to authenticate itself to the data center if needed. In mailing applications this may not be needed.

After such authentication, if it is desired, the data center 112 transmits a rate table and/or calculation algorithm. This transmission, however, requires a data integrity. That is, that the rate table and/or calculation algorithm should arrive unmodified. Assurance is needed that the rate table and/or calculation algorithm arrives exactly as it was sent and that it has not been corrupted, intentional or unintentionally. In order to accomplish this, the data center 112 first generates a hash value (message digest) of all or some specified portion of the data contained in the rate table and/or of the calculation algorithm to be sent. The rate table and/or calculation algorithm can then be sent as an ASCII or other type of file. The hash function applied to this data produces a hash value (message digest) which is indicative of the content of the rate table and/or calculation algorithm and yet is considerably reduced in data size. As used herein hash function is a well known function which possesses at least two properties. It is computationally difficult to (i) recover a message corresponding to a given message digest and (ii) to find two different messages which produce the same hash value (message digest). Some well known hash functions are described in American National Standard X9.30 - 1993, Public Key Cryptography Using Irreversible Algorithms For The Financial Services Industry: Part 2: The Secure Hash Algorithm (SHA). It should be noted that there are other publicly available hash functions that can be implemented for the purpose of the present invention. As for example, one formal definition is set forth in Contemporary Cryptology by G. Simmons, IEEE Press 1992 at page 345, and yet another definition is that a hash function h is a function that satisfies the following properties: 1) it is capable of converting a file F of arbitrary length into a fixed-length digest h (F); 2) h must be "one way", that is, given an arbitrary value y in the domain of h, it must be computationally infeasible to find file F such that h (F) = y; and 3) h must be "collision free", that is, it must be computationally infeasible to construct two different files F_1 and F_2 such that h (F_1,) = h (F_2).

Since the data (the rate table and/or calculation algorithm) being transmitted to the postage evidencing device 112 is publicly available information, it is not necessary to encrypt the information and prevent unauthorized decryption since it is not important to protect secrecy of the information itself. Upon calculation of the hash value (message digest) of the rate table and/or the calculation algorithm the data center encrypts the hash value (message digest) with its secret key (for both public and secret key systems) and sends the encrypted message to the postage evidencing device 114. The postage evidencing device 114 receives the encrypted hash value ("signature"), and decrypts it with its secret or public key as the case may be, thus obtaining the plaintext hash value (message digest). The postage evidencing device 114 then independently computes the hash value (message digest) of the received rate table and/or calculation algorithm using the same hash function. The hash algorithm employed may be one in the public domain; however the algorithm resides both at the data center 112 and at the postage evidencing device 114. If the two hash values received from the data center and the hash value computed in the postage evidencing device match each other, the integrity of the rate table received and stored in the postage evidencing device rating module 116 is assured. Thus, the integrity of the stored rate table and/or calculation algorithm is verified.

Both steps (authentication of the data center and verifying the integrity of the rate table and/or calculation algorithm received) can be combined. To do so, the data center 112 simply sends two messages to the postage evidencing device 114: the rate table and/or calculation algorithm in plain text and the rate table and/or calculation algorithm encrypted with the secret key. Thus, the authenticity of the sender and the verification of the message can be achieved in one step.

A description now follows in connection with FIGURES 2, 3 and 4 of the activities of a rate table/calculation algorithm at the data center 112 and at the postage evidencing device 114.

Reference is now made to FIGURE 2. The data center 112 sends the rate table and/or calculation algorithm to the postage evidencing device 114 at 214. Thereafter, the data center 112 computes the hash value (message digest) of the rate table at 216. The hash value is then encrypted by the data center 112 at 218. The encrypted hash value is transmitted to the postage evidencing device 114 at 220.

Reference is now made to FIGURE 3. The rate table is received by the postage evidencing device 114 at 322. The postage evidencing device 114 also receives the encrypted hash value of the rate table at 324. The

the hash values (message digest) match, verification is established, which means that an uncorrupted rate table was used for the rating process. The rate value together with the rate table identification are retrieved and sent to a postal revenue block formatting routine for formatting the data for printing.

The flow chart in FIGURE 4 shows the activities in the postage evidencing device 114 for rating a mail piece and printing the appropriate postage payment on the mail piece 124.

Reference is now made to FIGURE 4. A user enters rating parameters into the postage evidencing device 114 at 438. The postage evidencing device 114 verifies the consistency of the mail piece parameters at 440. A verification message is then sent at 442. If consistency has not been established at 443, the mail piece is rejected at 445. If consistency has been established at 443, the rate is computed at 444.

As part of computing the rate, the rate table and rate table calculation (computation) algorithm are authenticated at 446. An authentication message is sent at 448. If authentication has not been established at 450, the rate table is rejected at 452 and the process is not allowed to proceed. Thus, the rate computation noted above will not occur. If the authenticity of the rate table has been established at 450, the computation at 444 is enabled based on the authenticated rate table and on the verified mail piece parameters. The computed rate is sent to the postage printing formatting module at 447.

Reference is now made to Figure 5. The activities within the postage evidencing device 114 relating to authenticating the rate table as shown in Figure 4, block 444 involves a series of steps. Initially, after receiving the verification message of consistency of the mail piece parameters, a pointer is computed to the rate table based on the parameters at 544. The hash value (message digest) of the rate table is computed at 546. The computed hash value (message digest) of the rate table is compared with the hash value (message digest) of the rate table stored in the postage evidencing device non-volatile memory at 548. If the hash values do not match at 548, the process is stopped at 549 and various alternatives can be implemented as previously noted including locking up the postage evidencing device, allowing the number of lead tries or setting a flag in the postage evidencing device NVM.

If the hash values (message digest) match at 548, access to the rate table itself is enabled at 550 and the rate involved is obtained. The rate is formatted as part of the revenue block enabling the postage evidencing device to be prepared to print at 552. The postage evidencing device printer 122 is then enabled for printing at 554 and printed at 556. The formatting of the postal revenue block will include the hash value (message digest) as well as the rate to enable later identification. All or a part of the information contained in the hash value can be utilized to determine the authenticity, validity, and currency of the rate table. Moreover, the rating vectors (rating parameters) are also printed. As previously noted the hash value may be encrypted or parameterized by a secret key. This prevents the use, for example, of improper rating vectors or rate table and the deliberate altering of the hash value or part thereof for the proper rating vectors and proper rate table.

Reference is now made to Figure 6 which is a representative mail piece with one example of the type of information which may be printed on the mail piece 124. It should be recognized that the printed information and its organization are a matter of choice and can be printed at different locations on the envelope panel or tape; moreover, the information relative to a mail piece may be stored with a mail piece and/or mailer identifier code for later processing and analysis. The stored data for later analysis can be for a single mailer or a group of mailers. The data will provide information concerning mailing patterns and information regarding rating experience for any such mailer or group of mailers.

The formatted printed postal revenue block in the present example includes a postage evidencing device identification number 612, a town circle 614, and a postage amount and suitable indicia design which may include graphics of which could change with the value and the amount 616.

Printed at the bottom of the postage printing block 600 is a sequence of information segments including the hash value or part thereof (message digest of the rate table and/or calculation algorithm 618). As noted this hash value may be encrypted or parameterized. This value provides identification of the rate table itself and/or calculation algorithm, as previously described. The weight classification of the mail piece is printed at 620 and the desired level of service is printed at 622 (one day delivery, three day delivery, 6 day delivery, etc.). The class of service, for example, registered mail,is printed at 624 and a flag for oversized mail piece is printed at 626. A workshare level such as presort, barcoding, etc., is printed at 628.
To facilitate rapid scanning of the printed information a barcode representation of some or all of the information previously noted is printed at 630.

It should be clearly recognized that the information printed, its location, the fonts used, the bar code types and styles are all a matter of design choice and can be modified to meet the needs and requirements of the particular postal service or private carrier or mailer involved, depending upon the conventions established for these matters. Moreover, the problem of checking of stores and retrieves from a memory such as a RAM is known in the art (see for example Checking The Correctness of Memory, by M. Blum, et al, Proceedings of the IEEE Symposium Foundations of Computer Science, Pages 90-99, 1991).

reporting of funds printed by the postage evidencing device since last audit) and may be encrypted to prevent tampering. The postage evidencing device 114 would reverify the rate table using the new hash value as part of the funds reset process. If the new hash value does not match the hash value computed from the resident rate table, no postage printing would be allowed. In an alternate arrangement, the postage evidencing device 114 would calculate the hash value in the current rate table and upload the device current rate table hash value to the data center before any funds recharging or other funds transaction is authorized. If the hash value from the postage evidencing device does not match the hash value calculated at the data center, no additional funds recharging (or the funds transaction) would be authorized by the data center. In either arrangement, the postage evidencing device 114 can display a message to the user indicating that updating the rate table is required.

It should be recognized that, rather than requiring the updating of the rate table or reverification of the rate table to be part of a recharging or other funds transaction, the requirement can be based on a calendar clock resident in the postage evidencing device 114. Thus, after a predetermined period of time, as for example twenty four hours, forty eight hours, seventy two hours or any other selected time period, the meter can become inoperative until a reverification that current rate tables are being utilized. In yet another arrangement this reverification can be at a point where particular value of postage has been printed or after a certain number of power up, power down cycles.

By requiring the uploading or recomputation of rate tables it is also possible to determine whether the rate table resident within the postage evidencing device has been tampered with because of the lack of appropriate hash value for either a current rate table or a previously valid rate table. In such case, meter operation can be inhibited either by the failure to enable recharging of the meter or by downloading a data code which inhibits operation of the meter.

It should still be understood that the arrangement described above in connection with insuring the integrity of the data loaded into the postage evidencing device 114 can be mailing data other information within the postage evidencing device 114 or peripherals to the postage evidencing device. For example, if a mailing list is downloaded into the postage evidencing device by the techniques described above, the hash values can be computed during the operation to insure the data was not corrupted during the loading process or the utilization of the data during operation of the postage evidencing device. The hash values can be generated each time a specified number of transactions (of any type) occur. The hash values would be stored in the postage evidencing or in the data center or other data repository. A postal service or a carrier or other party would thereby be able to detect and determine corruption of the data by querying the postage evidencing device or peripheral. The sequence of hash values stored would allow a determination of when and where tampering occurred depending on the nature of the parameters used to generate the hash value.

While the present invention has been disclosed and described with reference to the specific embodiments described herein, it will be apparent that variations and modifications may be made therein.

ceived rate table stored in said rating device non-volatile memory; and
means for comparing the received hash code with the generated hash code.

2. A postal rating system as defined in claim 1 wherein said transmitted hash code is an encrypted hash code and including means in said rating device for decrypting the encrypted hash code and comparing the decrypted hash code with the generated hash code.

3. A postal system as defined in claim 2 wherein the received hash code and the generated hash code are each based upon the entire rate table.

4. A postal system as defined in claim 2 wherein said transmitted hash code and said transmitted rate table each includes data as to the time period when the rate table is valid.

5. A postage evidencing device comprising:
means for storing a postal rate table in a non-volatile memory;
means for storing a hash code based on information from the rate table in said non-volatile memory;
means for receiving a request for printing of postage value;
means for recomputing the hash code from said information from said rate table stored in said non-volatile memory;
means for comparing the recomputed hash code based with said hash code stored in said non-volatile memory; and
means for comparing said recomputed hash code and said stored hash code.

6. A postage evidencing device as defined in claim 5 further including:
means for printing at least one of said stored and said recomputed printing hash codes on a mail piece;
means for printing said mail piece rating parameters on said mail piece such that a verifying party can reconstruct the rating process and determine if rating inaccuracy occurred.

7. A postage evidencing device as defined in claim 6 further including means for encrypting said hash code such that said printing means is enabled to print an encrypted hash code on said mail piece.

8. A system for verifying the accuracy of postal rating, comprising:
means for scanning a mail piece to detect a hash code printed on a mail piece and rating parameters also printed on the mail piece;
means for recomputing the rating process to determine the rating accuracy; and,
means for determining the correctness of said rating for said scanned mail piece.

9. A system as defined in claim 8 further including means for storing a profile of a mailer based on information from said determining means to provide data concerning rating activities for a series of mail pieces.

10. A mail piece having imprinted thereon a postal rate based on a postal rate table, the improvement comprising imprinting on said mail piece a code based on information derived from the postal rate table and which provides an identification of the rate table.

11. A mail piece as defined in claim 10 wherein said code imprinted on said mail piece is a value derived from processing said rate table information with a function which precludes recreating said rate table information based solely on said imprinted value.

12. A mail piece as defined in claim 10 wherein said code is encrypted.

13. A mail piece as define in Claim 11 wherein said function is a hash function.

14. A mail piece as defined in claim 13 wherein said code is encrypted.

15. A mail piece as defined in claim 13 wherein said code imprinted on said mail piece is related to a hash value.

16. A mail piece as defined in claim 15 wherein said code is an encrypted hash value.

include data as to the rate table validity time period.

36. A postal rating system comprising:
a postal rating device having secure storage means;
means for transmitting a postal rate table to said postal rating device such that said postal rate table is stored in said rating device secure storage means;
means for transmitting to said postal rating device a hash code such that said hash code is stored in said rating device secure storage means, said hash code based on information from said rating table;
means in said postal rating device for generating a hash code based on information from said received rate table stored in said rating device secure storage means memory; and
means for comparing the received hash code with the generated hash code.

37. A postal rating system as defined in claim 36 wherein said transmitted hash code is an encrypted hash code and including means in said rating device for decrypting the encrypted hash code and comparing the decrypted hash code with the generated hash code.

38. A postal system as defined in claim 37 wherein the received hash code and the generated hash code are each based upon the entire rate table.

39. A postal system as defined in claim 37 wherein said transmitted hash code and said transmitted rate table each includes data as to the time period when the rate table is valid.

40. A method of printing postage evidence, comprising the steps of:
storing a postal rate table;
storing a code based on information from the rate table;
receiving a request for printing of postage value;
recomputing the code from said information from said stored rate table; and
comparing said recomputed code and said stored code.

41. A method as defined in claim 40 wherein said stored code and said recomputed code are each hash codes.

42. A method of printing postage as defined in claim 40 further including the steps of:
printing said code on a mail piece; and,
printing said mail piece rating parameters on said mail piece to enable reconstruction of the rating process from information imprinted on said mail piece.

43. A method as defined in claim 42 wherein said code is encrypted and said encrypted code is printed.

44. A method as defined in claim 40 further including printing a postage rate, printing the date of printing the postage rate and printing said code on said mail piece, said code containing data as to the time period when said rate table is valid.

45. A method as defined in claim 44 wherein said code is encrypted and said encrypted code is printed.

46. A method for a mailing system, comprising the steps of:
generating a request for recharging a postage evidencing device with additional postage value to be printed;
determining the validity of a rate table associated with said postage evidencing device; and,
enabling recharging of said postage evidencing device if said rate table is determined to be valid.

47. A method as defined in claim 46 wherein said steps of determining includes said postage evidencing device transmitting to a remote location a hash code value of a rate table currently associated with said postage evidencing device.

48. A method as defined in claim 46 wherein said steps of determining includes transmitting to said postage evidencing device a hash code value of a currently valid rate table.

49. A method for a mailing system, comprising the steps of:
determining the validity of a rate table associated with a postage evidencing device; and
enabling operation of said postage evidencing device if said rate table is determined to be valid.

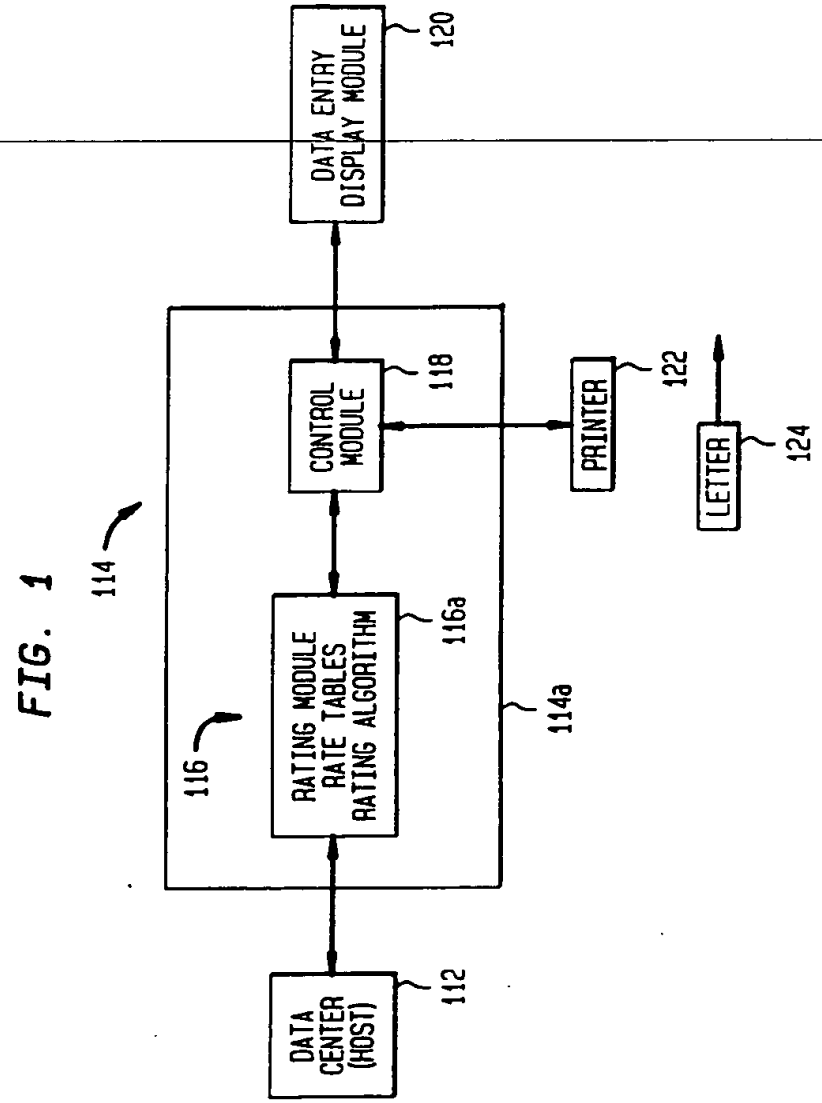


FIG. 1

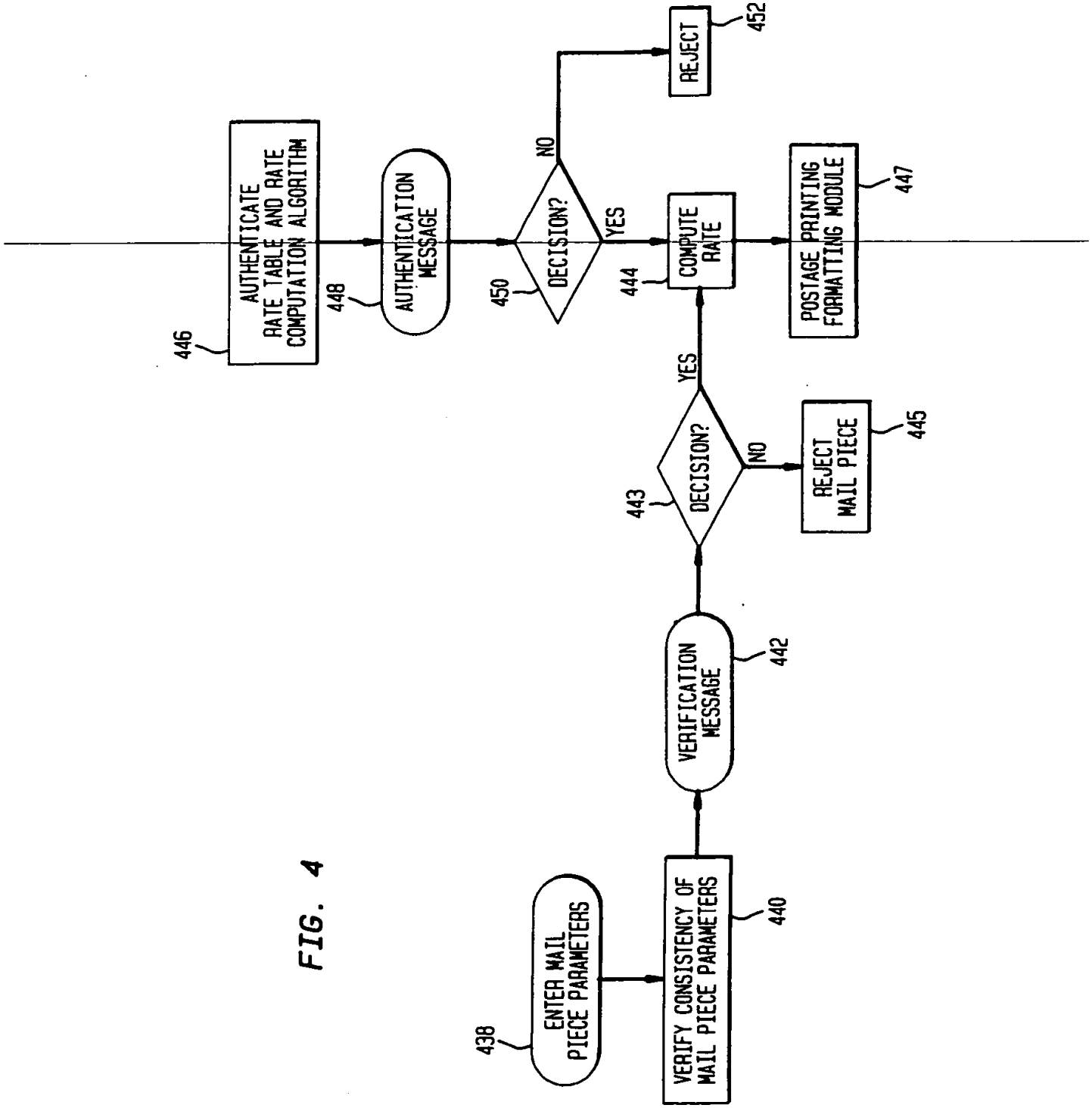
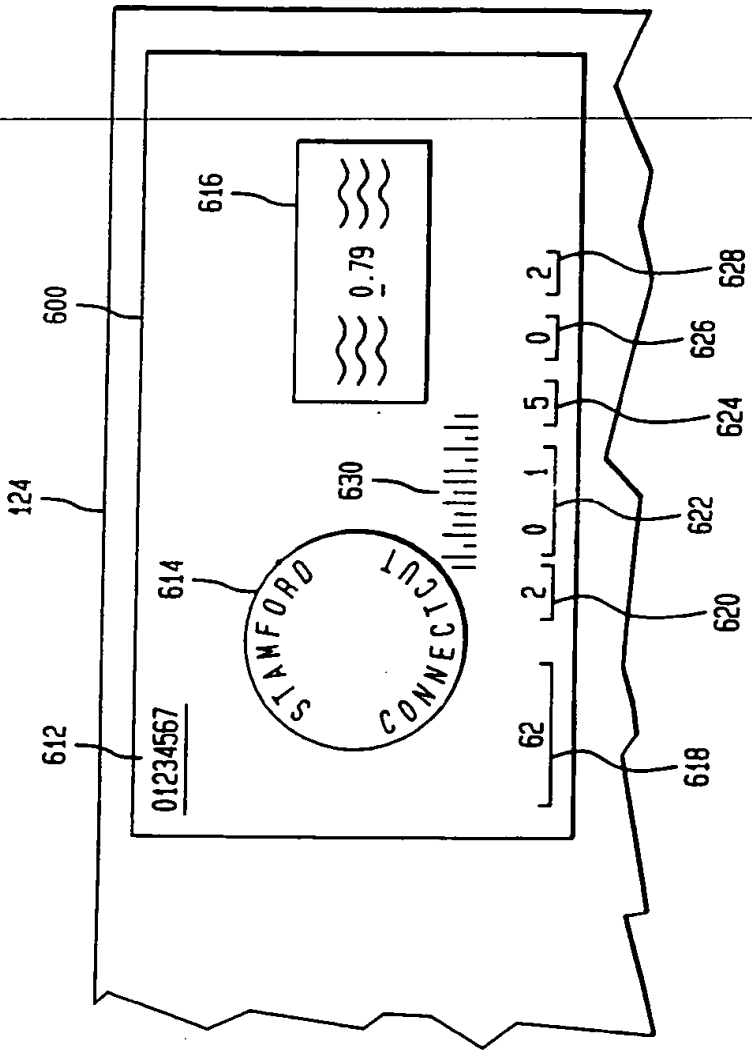


FIG. 4

FIG. 6



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 647 925 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **94307376.7**

(51) Int. Cl.[6] : **G07B 17/04**

(22) Date of filing : **07.10.94**

(30) Priority : **08.10.93 US 133398**

(43) Date of publication of application :
12.04.95 Bulletin 95/15

(84) Designated Contracting States :
CH DE FR GB LI

(88) Date of deferred publication of search report :
25.10.95 Bulletin 95/43

(71) Applicant : **PITNEY BOWES, INC.**
World Headquarters
One Elmcroft
Stamford Connecticut 06926-0700 (US)

(72) Inventor : **Pintsov, Leon A.**
365 Mountain Road
W. Hartford, Connecticut 06107 (US)
Inventor : **Connell, Richard A.**
24 Lower Salem Road
South Salem, New York, 10590 (US)
Inventor : **Sansone, Ronald P.**
4 Trails End Road
Weston, Connecticut 06883 (US)
Inventor : **Schmidt, Alfred C.**
201 Branch Brook Road
Wilton, Connecticut 06897 (US)

(74) Representative : **Cook, Anthony John et al**
D. YOUNG & CO.
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Postal rating system with verifiable integrity.

(57) A data center provides a rate table to a user. The rate table is communicated to the mailer along with a hash code. The hash code is based on information from the rating table. The hash code provides a unique number based on the rating table provided. The algorithm within a secure device and to which the rate table is loaded regenerates the hash code based on the information received from the rate table and compares the transmitted hash code with the generated hash code. A comparison is made of the received hash code and the generated hash code to verify that the rate table data has not been intentionally or unintentionally corrupted. The transmitted hash code may be encrypted by the data center and when received decrypted by the mailer. The encryption decryption process establishes authenticity of the data center if desired.

The generation of a hash code based on the stored rate table and a comparison with a stored hash code previously transmitted can be initiated prior to postage printing and used to insure proper rating. Printing is enabled only after the rating process has been properly implemented. The hash code and rating information may be printed on the mail piece such that a verifying party can reconstruct the rating process and determine if rating inaccuracy occurred. Various rating inaccuracy for a particular user can be stored by the verifying party to detect a recurrence of rating errors. Rating profiles for particular users or group of users may be stored to enable generation of user profiles.

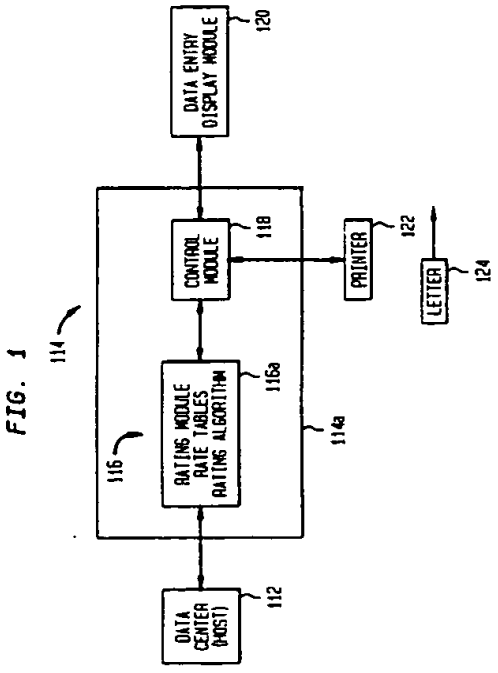


FIG. 1

EP 0 647 925 A3